Prior to examination of the above-captioned application, kindly enter the following Amendment:

IN THE CLAIMS:

Please cancel claims 2-82 without prejudice or disclaimer of the subject matter thereof.

Please add claims 83-163 as follows:

83. A method for an authority to authenticate certificate information provided to a intermediary in a manner that enables an end user to verify portions of the information, comprising:

(a) mapping the information into a plurality of certificate values;

(b) constructing an authenticated tree having an authenticated root and having certificate nodes corresponding to the certificate values;

(c) the intermediary obtaining the authenticated root and at least one of the certificate nodes; and

(d) the intermediary causing the end user to receive verification data including at least one of: the authenticated root, one of the certificate nodes, and one of the node values of the authenticated tree;

(e) the end user verifying the certificate using at least a portion the verification data.

84. A method according to claim 83, wherein the intermediary obtains the authenticated root and at least one of the certificate nodes from the authority.

85. A method according to claim 83, wherein the end user receives the authenticated root from the intermediary.

86. A method according to claim 83, wherein the end user receives the authenticated root from the authority.

87. A method according to claim 83, wherein the end user receives the authenticated root from the authority.

88. A method according to claim 83, wherein the end user receives at least one of the certificate nodes from the intermediary.

89. A method according to claim 83, wherein the root is authenticated with a digital signature.

90. A method according to claim 89, wherein the digital signature is verifiable by the end user.

91. A method according to claim 83, wherein the certificate values indicate which certificates have been revoked.

92. A method according to claim 91, wherein the certificate values include a date of revocation for the certificates that have been revoked.

93. A method according to claim 83, wherein the certificate values indicate which certificates are valid.

94. A method according to claim 93, wherein the certificate values include a date of expiration for the certificates that are valid.

95. A method according to claim 83, wherein the certificate values indicate which certificates have been issued.

B1 Cont'

96. A method according to claim 95, wherein the certificate values include a date of issue for the certificates that have been issued.

97. A method according to claim 83, wherein the certificate values indicate which certificates have been revoked and which certificates are valid.

98. A method according to claim 83, wherein the certificate values indicate which certificates have been revoked and which certificates have been issued.

99. A method according to claim 83, wherein the certificate values indicate which certificates are valid and which certificates have been issued.

100. A method according to claim 83, wherein the certificate values indicate which certificates have been revoked, which certificates are valid, and which certificates have been issued.

101. A method according to claim 83, wherein values of the internal nodes are obtained by performing a one-way hash of the values of the children thereof.

102. A method according to claim 101, wherein the value of at least one of the internal nodes is obtained by performing a one-way hash of a combination of the values of the children of the internal node and a value of the internal node.

103. A method according to claim 102, wherein the value of the internal node indicates a position of the internal node within the tree.

104. A method according to claim 83, wherein at least one of the certificate nodes corresponds to more than one certificate.

105. A method according to claim 83, wherein mapping and constructing are performed by the authority.

106. A method according to claim 91, wherein mapping and constructing are performed by the authority.

107. A method according to claim 83, wherein certificate information determines locations of the nodes within the authenticated tree.

108. A method according to claim 83, wherein the certificate information determines the certificate nodes corresponding to the certificate values mapped from the certificate information.

109. A method according to claim 108, wherein positions of nodes within the authenticated tree provide at least a portion of the certificate information.

110. A method according to claim 109, wherein the certificate information includes serial numbers for each of the certificates.

B1 CONT'

111. A method according to claim 106, wherein the certificate information relates to certificates having serial numbers that determine the certification nodes.

112. A method according to claim 106, wherein the authority also revokes certificates.

113. A method according to claim 95, wherein mapping and constructing are performed by the authority.

114. A method according to claim 113, wherein the authority also issues certificates.

115. A method according to claim 83, wherein the certificate values correspond to serial numbers of the certificates.

116. A method according to claim 115, wherein the certificate values correspond to serial numbers of the certificates combined with additional information.

117. A method according to claim 83, wherein the authenticated root contains additional information.

118. A method according to claim 117, wherein the additional information includes date information.

119. A method according to claim 117, wherein the additional information includes an indication of at least one of: revoked, issued, and valid for describing the certificate information corresponding to the certificate nodes of the authenticated tree.

120. A method according to claim 83, wherein the certificate nodes are leaf nodes of the authenticated tree.

121. A method according to claim 83, wherein the intermediary causes authenticating values of at least one of the certificate nodes to be provided to the end user.

122. A method according to claim 83, wherein the certificate information includes serial numbers of the certificates.

123. A method according to claim 122, wherein location of the certificate nodes within the authenticated tree varies according to the certificate values.

124. A method for a intermediary to prove to an end user that certificate information is authenticated by an authority, comprising:

(a) obtaining at least a portion of an authenticated tree having certificate nodes corresponding to certificate values indicative of the information; and

(b) causing the end user to receive at least one of the following values: certificate values, authenticating values of certificate values, and one or more node values authenticated by an authority.

B1 Cont.

125. A method according to claim 124, wherein at least one of the authenticated node values is the root value.

126. A method according to claim 124, wherein the user receives at least one of: a certificate value, a node value, and an authenticated node value.

127. A method according to claim 124, wherein the user uses at least a value that the intermediary caused the user to receive to verify the authenticity of the certificate information

128. A method according to claim 127, wherein the end user verifies the authenticity of the certificate information via an authentication path of at least one certificate node

129. A method according to claim 124, wherein the authenticated tree values and the authenticated node values change over time.

130. A method according to claim 124, wherein the intermediary sends at least one of: a certificate value, a node value, and an authenticated node value.

131. A method according to claim 124, wherein the intermediary can prove to the user that a certificate information does not correspond to a certificate that was issued.

132. A method according to claim 124, wherein the intermediary can prove to the end user that a given serial number does not correspond to any issued certificate of a given CA.

133. A method according to claim 124, wherein the certificates are public key certificates.

134. A method for a intermediary to prove to an end user that certificate information is authenticated by an authority, comprising:

(a) obtaining an authenticated tree having certificate nodes corresponding to certificate values indicative of the information;

(b) obtaining an authenticated root of the authenticated tree, wherein the authenticated root proves that the authority authenticated the tree;

(c) causing the end user to receive certificate values and to receive authenticating values of certificate values; and

(d) causing the end user to receive the authenticated root, whereby the authenticated root and authenticating values are used by the user to verify the certificate values.

B1 Cont'

135. A certificate revocation system in which one or more authorities issue and revoke certificates and an intermediary provides end users certificate information authenticated by the one or more authorities having the intermediary prove to an end user that a given certificate has not been issued by a given authority by a given date by providing a piece of information generated by the given authority.

136. A certificate revocation system, according to claim 135, wherein the piece of information includes a digital signature of the authority.

137. A certificate revocation system, according to claim 136, wherein the piece of information can be verified by the end user in conjunction with a separate piece of information generated by the authority.

138. A certificate revocation system, according to claim 137, wherein the separate piece of information includes a digital signature of the authority

139. A certificate revocation system, according to claim 138, wherein the piece of information includes at least one value of a node in an authenticated tree.

140. A certificate revocation system, according to claim 139, wherein the separate piece of information is the authenticated root of the authenticated tree.

B1 CONT.

141. A method for authenticating certificate revocation information about a plurality of certificates, each having a certificate identifier belonging to a set of possible identifiers, comprising:

(a) for all of the certificate identifiers, mapping the revocation information into a plurality of certificate revocation values;

(b) constructing a tree having certificate nodes containing the certificate revocation values, wherein, for each possible certificate identifier, the tree is guaranteed to contain at least one node having a certificate revocation value indicating whether a certificate corresponding to the certificate identifier is revoked;

(c) storing values within internal nodes of the tree, wherein the values stored in the internal nodes authenticate values contained in children thereof; and

(d) authenticating a root certificate node of the tree to provide an authenticated root.

142. A method according to claim 141, wherein an intermediary obtains the authenticated root and at least one of the certificate nodes from an authority that authenticates the root.

143. A method according to claim 142, wherein an end user receives the authenticated root from the authority.

144. A method according to claim 143, wherein the end user receives at least one of the certificate nodes from the authority.

145. A method, according to claim 144, wherein the root is authenticated with a digital signature.

146. A method according to claim 145, wherein the digital signature is verified by an end user.

147. A method according to claim 141, wherein the certificate nodes are leaf nodes of the tree.

148. A method according to claim 141, wherein an intermediary causes authenticating values of at least one of the certificate nodes to be provided to an end user.

149. A method according to claim 141, wherein an intermediary constructs the tree.

150. A method according to claim 141, wherein an authority constructs the tree.

151. A method for authenticating certificate revocation information about a plurality of certificates, each having a certificate identifier belonging to a set of possible identifiers, comprising:

(a) for all of the certificate identifiers, mapping the revocation information into a plurality of certificate revocation values;

(b) constructing at least one tree having certificate nodes containing the certificate revocation values, wherein, for each possible certificate identifier, the at least one tree is guaranteed to contain at least one node having a certificate revocation value indicating whether a certificate corresponding to the certificate identifier is revoked;

(c) storing values within internal nodes of the at least one tree, wherein the values stored in the internal nodes authenticate values contained in children thereof; and

(d) authenticating a root certificate node of the at least one tree to provide an authenticated root.

152. A method according to claim 151, wherein an intermediary obtains the authenticated root and at least one of the certificate nodes from an authority.

153. A method according to claim 152, wherein the certificate nodes are leaf nodes of the at least one tree.

154. A method according to claim 151, wherein the certificate values include a date of issue for the certificates that have been issued.

155. A method according to claim 151, wherein the end user receives the authenticated root from an intermediary.

156. A method according to claim 151, wherein the end user receives the authenticated root from an authority.

157. A method according to claim 151, wherein an end user receives the authenticated root from an authority.

158. A method according to claim 151, wherein an end user receives at least one of the certificate nodes from an intermediary.

159. A method according to claim 151, wherein the root is authenticated with a digital signature.

160. A method according to claim 159, wherein the digital signature is verifiable by the end user.

161. A method according to claim 151, wherein the certificate values indicate which certificates are valid.

162. A method according to claim 161, wherein the certificate values include a date of expiration for the certificates that are valid.